Policy on E-Safety

We are living in an increasingly connected technological world where, alongside the benefits of access to technology, come increased risks to children. Lack of guidance and learning in E-safety can mean children are unaware of the unintended consequences of their online behaviour or actions. It highlights the need to educate our children and the school community about the benefits and risks of using Internet technologies and electronic communications, and provide safeguards and awareness for users, to enable them to keep safe and to control their online experience.

Our aim is to make the children at The Hendreds School as safe and productive in the online world, both in school and outside of school, as they are in the real world with particular focus on protection against cyberbullying and grooming.

This policy is intended for our children, staff, parents, governors, volunteers and visitors.

What is E-Safety?

E-safety is a school's ability to protect and educate its children and staff in their use of technology as well as having appropriate mechanisms in place to respond to and support any incident where appropriate. At The Hendreds, we aim to protect and educate our children and will respond to incidents where children's safety may be at risk.

Protecting children means providing a safe learning environment by using appropriate monitoring and filtering to control what children can access while at school. Education around e-safety is the only way to ensure that, wherever they are, they know how to stay safe online.

Learning about e-safety is a vital life skill. Empowering children at an early age with the knowledge to safeguard themselves and their personal information is something that needs to be nurtured throughout school to see them into adult life. Equally, it is important to empower adults, particularly parents, with the right information so that they can identify risky behaviour, or mitigate the possibility of risk.

The school's E-safety covers a wide range of aspects, including:

- Online behaviour – understanding what constitutes cyber-bullying, inappropriate content and how to behave safely and with respect for others.
- Protecting your online reputation – understanding both the risks and rewards of sharing personal information online (your digital footprint).
- Learning to evaluate internet content – understanding how to research, evaluate and use published material.

The internet is an essential aspect of learning across all walks of life. In school, access to the internet is essential to:

- Raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management functions.
- Prepare children for life in the 21st century in terms for education, business and social interaction. The school has a duty to provide children with quality and safe internet access as part of their learning experience.
- Teach children how to evaluate internet information and to understand and to take care of their own safety and security.

There are many benefits of the internet to learning:

- Access to world-wide educational resources
- Collaboration and communication between children
- Access to anytime, anywhere learning
- Access to experts in many fields for children and staff
- Professional development for staff through access to national developments, educational materials and example of effective curriculum practice
- Collaboration across support services and professional associations
- Improved access to technical support including remote management of networks and automatic system updates
- Exchange of information

With increased use of the internet, protecting and educating children to manage the risk becomes our primary concern. As a school we commit to provide parents with support and information in keeping children safe online.

Children

The school has a clear 'Acceptable Use Agreement for Children' which forms the code of conduct. To support appropriate access to the internet and use of electronic communications, we ensure that:

- The E-safety Policy is published on the school website
- Children are informed and are aware that internet use is monitored
- E-safety is delivered to raise the awareness and importance of safe and responsible use of the internet and other electronic communication tools. This is delivered in the classroom through relevant lessons and PSHE sessions, and beyond the classroom through structured annual training and specially focused input from outside providers. E-safety messages are reinforced each time internet access or ICT usage is given.

Staff

As standard practice we ensure that:

- All staff are given the School E-safety Policy and its application and importance explained
- Staff are asked to read and sign the 'Acceptable Use Agreement for Staff'
- Staff are fully aware that internet traffic can and will be monitored and traced to the individual user. Discretion and professional conduct is essential

Parents

Internet use in the home is increasing rapidly. Parents need to aware of the dangers and ensure all technological equipment used in the home has the required and appropriate level of age appropriateness and software protection. As a school, we recognise the importance of striking a careful balance between informing and alarming parents. Our policy is to:

- Draw parents' attention to E-safety resources in particular the school's E-safety Policy, relevant articles and resources from trusted sources, and online reporting procedures in newsletters and on the school website
- Handle internet issues sensitively, to inform parents without alarm
- Encourage a partnership approach with parents where careful and informed practise can be supported in and out of school. This includes professionally delivered parent E-safety information sessions that build awareness of benefits and risks, and offer independent advice and best practice suggestions for safe home Internet and e-communications use. In addition to this, useful links are included in the parents section on the school website

Governing Body

All Governors of the school are expected to understand, uphold and ensure E-safety best practice for staff and children. As internet and communication access broadens, so governors must ensure that the school keeps pace in its policies and procedures and can effectively protect, educate and respond.

School

School has a range of strategies and policies to prevent online bullying, these include:

- No access to public chat-rooms, instant messaging services and bulletin boards.
- Children are taught how to use the internet safely and responsibly and are given access to guidance and support resources from a variety of sources. Specific education and training on cyber bullying (understanding what behaviour constitutes E-Safety Policy, cyberbullying and its impact, how to handle concerns and report incidents) is given as part of an annual visit from the Life Bus.
- Children are encouraged to discuss any concerns or worries they have about online bullying and harassment with staff.
- Children are informed on how to report cyber bullying.
- Complaints of cyber bullying are dealt with in accordance with our Behaviour and Discipline Policy.
- Complaints related to child protection are dealt with in accordance with school child protection procedures.

Grooming

Grooming is a word used to describe how people gain the trust of children - and possibly their families - with the intention of potentially harming them. Online grooming may occur by people forming relationships with children and pretending to be their friend. They do this by finding out information and seeking to establish false trust. The school has measures in place to educate and protect children against this risk. These include:

- No access to public chat-rooms, instant messaging services and bulletin boards. Children do not have access to their mobile phones during the school day.
- All online access and children generated content in school is monitored and password protected
- Children are taught how to behave responsibly online and the rules in protecting personal information
- Children, staff, parents and governors are provided with appropriately targeted training on risks and solutions to keep safe online

Authorising Internet Use
Children are expected to complete the E-Safety Code of Conduct and are authorised to access the internet as a group or independently, depending on the activity. Internet usage is under the supervision of the teachers and teaching assistants. All staff read and sign the 'Staff Acceptable Use Policy'.

Managing Filtering
Our policy is that internet access must be appropriate for all members of the school community. Our ICT systems are managed by Turn It On, a company based in Witney. The procedures for ongoing management and review are:

- The school will work with Turn It On to ensure that systems are reviewed and any improvements needed are implemented
- If staff or children discover unsuitable sites, the URL must be reported to the Headteacher, who will then report this to Turn It On and ensure that the URL is blocked.
- Any material that the school believes to be illegal must be reported to appropriate agencies (IWF or CEOP)

Managing E-mail and Communications
All staff and Governors are given a secure school e-mail address. The creation of these accounts is the responsibility of the school administrator. Should any staff need to contact parents directly then they should use either the school telephone, their school e-mail, or communication should be passed through to the school office. All personal contact details for staff members will remain private.

Managing Published Content and Images
Our school website celebrates pupils' work, promotes the school, publishes resources and acts as a communication tool. Publication of information on the school website is carefully considered from a personal and school security viewpoint. Contact details available on the website are school address, e-mail and telephone number. Staff or pupils' personal information is not published and all images used will comply with the conditions below:

- Children's names are published as their first name only
- Staff are referred to by their title and surname
- Any images of children must not be labelled with their names.
- Children will only be shown in photos where they are suitably dressed.
- Completed consent forms from parents or carers must be obtained before images of pupils are electronically published. A master list is available and updated by the school office staff.

- While images may be taken by parents, it is requested that they are not shared in the public domain.
- All digital images are securely stored and disposed of in accordance with the Data Protection Act.

Managing Information Services

The Hendreds School is committed to take due care in regard to managing the provision of Information Services to support secure and appropriate access. The measures outlined in this Policy include:

- Network servers are kept securely in a locked room
- The security of the school information system is reviewed regularly
- The school reserves the right to monitor user areas and equipment provided by the school
- Sophos anti-virus software updates automatically every hour. Staff are also encouraged to install Sophos or any other secure protection at home to increase security
- The school uses Internet firewall and filters provided by Turn It On
- For fire safety network server backups of user data are taken daily and stored remotely using online servers.

Social Networking and Personal Publishing

Direct access to social networking sites is blocked in school. We recognise that children need guidance and support in knowing how to stay safe online whether in school or at home. Social networking sites have an age limit and it is the responsibility of parents to respect this and to ensure their children are complying with the regulations.

Children need to understand the dangers of uploading personal information and the practical impossibility of removing it. They need to be taught the reasons for caution in publishing personal information and photographs on the internet and in particular on social networking sites. Our E-safety Policy aims to provide guidance and on keeping safe within social networking and personal publishing.

- Children are advised never to give out personal details of any kind, which may identify them and / or their location. Examples would include real name, address, mobile or landline phone numbers, school attended,
- Children are advised not to place personal photos on any social network space. They should consider how public the information is and consider using private areas.
- Staff must ensure their profiles on social networking sites are private and not to add present or past pupils as friends.

We very much acknowledge that we cannot act in isolation and parent's co-operation in supporting these steps is greatly appreciated.

Risk Assessments

In line with commitments made within this policy, the school will take all reasonable precautions to ensure that users access only appropriate material. However, due to

the global and connected nature of internet content, it is not possible to guarantee that access to unsuitable material will never appear on a school computer. It is the responsibility of the school and staff to ensure our e-safety procedures are followed.

All internet access at The Hendreds School is protected under the filtering system set up by the company Turn It On. As part of our e safety procedures, children are taught to understand the risks of using the internet and how best to manage those risks. The Headteacher will ensure that the E-safety policy is implemented and compliance with the Policy monitored.

Mobile phones

Children are not allowed to have personal mobile phones or other similar devices in school. Parents may request that such devices are kept at the School Office or in the teacher's locked cupboard for children who may need them on their journey to and from school. However, in acknowledgement of the growing use, children will be taught about the benefits and risks, the legal and moral implications of posting photos and personal information from mobile phones to public websites, and how the data protection and privacy laws apply.

On-Line Behaviour

A critical part of our E-safety Policy which applies across all technologies is that teachers guide children to appropriate websites, or teach search skills. Information received via the Internet, e-mail, or text message requires good information handling skills. Our approach is to offer children a few good sites as this is often more effective than an internet search. Respect for copyright and intellectual property rights, and the correct use of published material are taught. Children need to learn to evaluate everything they read and to refine their own publishing and communications with others.

- The school internet access is designed expressly for children to use and includes filtering appropriate to the age of the children.
- Children are taught what internet use is acceptable and what is not and are given clear objectives for internet use.
- Internet access is planned to enrich and extend learning activities.
- Staff guide children in online activities that support the learning outcomes planned.
- ICT skills lessons are used to educate children in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation. This is reinforced by teachers when using the internet within their classroom.
- The school ensures that copying and subsequent use of the internet derived materials by staff and children complies with copyright law
- Children are taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy

E-Safety Contacts and References

Childnet International http://www.childnet.com/resources

Childline http://www.childline.org.uk

Think U Know (links to CEOP) www.thinkuknow.co.uk

Child Exploitation and Online Protection Centre www.ceop.gov.uk

Stop it now (child sexual abuse prevention campaign, for all adults) www.stopitnow.org.uk

Parents Protect www.parentsprotect.co.uk

E-Safety self-review tools provided by South West Grid for Learning
www.360safe.org.uk for schools and www.onlinecompass.org.uk for youth settings

Securus (Company supplying software to protect pupils from cyberbullying in schools)
www.securus-software.com

Internet Watch Foundation (IWF) www.iwf.org.uk was set up by the UK internet industry to provide the UK internet 'Hotline' for the public to report potentially illegal online content.

CBBC Stay Safe www.bbc.co.uk/cbbc/topics/stay-safe

Kidsmart http://www.kidsmart.org.uk/

NSPCC http://www.nspcc.org

Report it: Thames Valley Police – for suspected criminal activity
http://www.thamesvalley.police.uk/reptcr/reptcr-repform.htm

Oxfordshire County Council website – for child safeguarding concern
http://www.oxfordshire.gov.uk/cms/public-site/child-social-care

CEOP – report a child in danger of abuse. Children can self-report.
http://www.ceop.police.uk/safety-centre/

Virtual Global Taskforce – Report Abuse http://www.virtualglobaltaskforce.com/

Internet Watch Foundation – report child sexual abuse content http://www.iwf.org.uk/

Professionals Online Safety Helpline 0844 3814772